



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Scanning Networks – Part 2

/* This is a Continuation Activity – Complete Part 1 before starting this */



Activity 3 – Continuation

Objectives

In continuation to our earlier lectures, this tutorial helps in providing you an overview of tools used to scan and enumerate networks.

ETHICAL STATEMENT

The tools and techniques you are exposed to' in this lab is to work only on a virtual machine environment and the purpose is entirely to demonstrate various types of cyber-attacks. Experimentation with these tools, techniques, and resources is at the discretion of the instructor and institution. If you as a student consider using attack tools for educational purposes on an outside environment, you should contact me prior to any experimentation.

Note: Unauthorized access to data, computer, and network systems is a crime in many jurisdictions and often is accompanied by severe consequences, regardless of the perpetrator's motivations. It is the learner's responsibility, as the user of this material, to be cognizant of and compliant with computer use laws.

Part 1: Use HPING Version 3 to send ICMP/TCP/UDP Packets and analyse the target replies.

Part 2: Use MegaPing to identify live hosts and open ports of the Target.
--

Part 3: Use NetScanTools Pro to initiate various Scans

Part 4: Explore various network scanning Techniques
--

This activity will continue...

Part 5: Being Anonymous on the Internet
--

Part 6: Identify Target Operating System with TTL
--

Part 7: Map your Network

Part 8: Enumerate using NetBIOS
--

Part 9: Enumerate using Nmap and Net Use

ICONS Used in this document:



Find out the outcome/ Answers/ Solution



Do research and complete the task. Need referencing/ in-text citations.
Shall be included as a part of your coursework.



Record your Reflection

Part 5: Use Proxy Switcher to browse anonymously.

Machine: Windows Servers 2016/2012

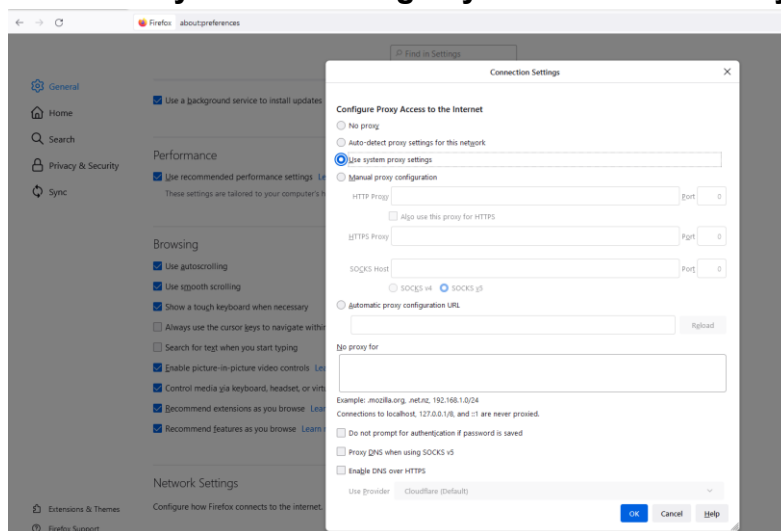
1. Download Proxy Switcher.

Which link did you use to download the tool? Why?

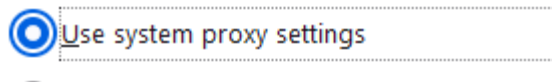


What is the purpose of this tool?

2. Install Proxy Switcher in Windows 2016. **USE ONLY IN LAB ENVIRONMENT**
3. Make sure you have changed your Browser's Proxy settings.



(This is in Firefox. Options varies in each browser. Look for Settings → Network Settings → Proxy)



4. Look at your public IP Address.

what is my ip address



Search Google or type a URL



Web Store



Add shortcut

whatismyip.com/my-ip-information/



WhatIsMyIP.com

IP Lookup

Speed Test

Change IP

Hide IP

Search ...

Sign Up

Login

WhatIsMyIP.com » Tools » My IP Information

My IP Information

Holidays just got easier

Book now

My Public IPv4 is:

2.96.16.17

Your IPv6 is: Not Detected



Stay safe, browse fast.

Get Special Deal

My IP Location Info

City: Bristol

State: England

Country: United Kingdom of Great Britain and Northern Ireland

My IP Hostname

ISP: TalkTalk Communications Limited

Host Name: host-2-96-16-17.as13285.net

ASN: 13285

What is your IP Address?



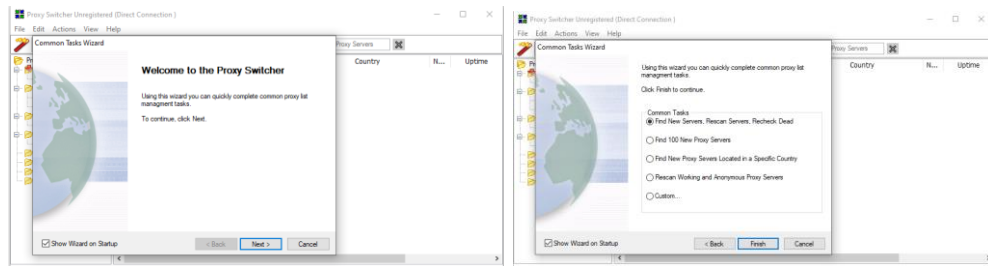
What is your location?

Could you locate/see any proxy detected?

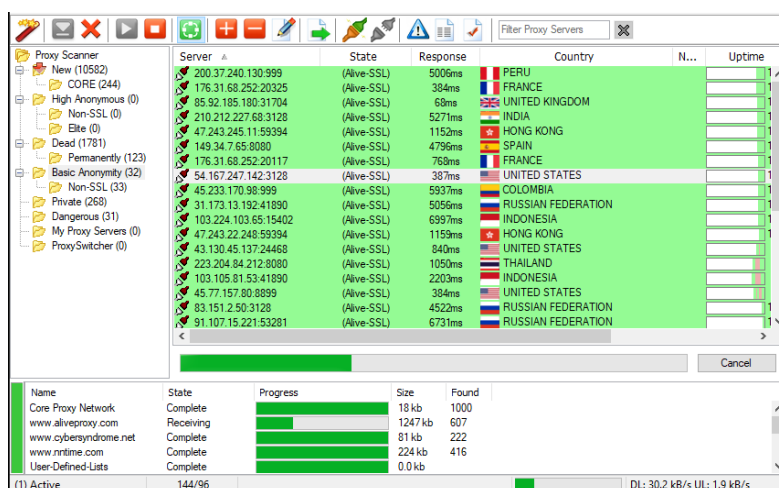
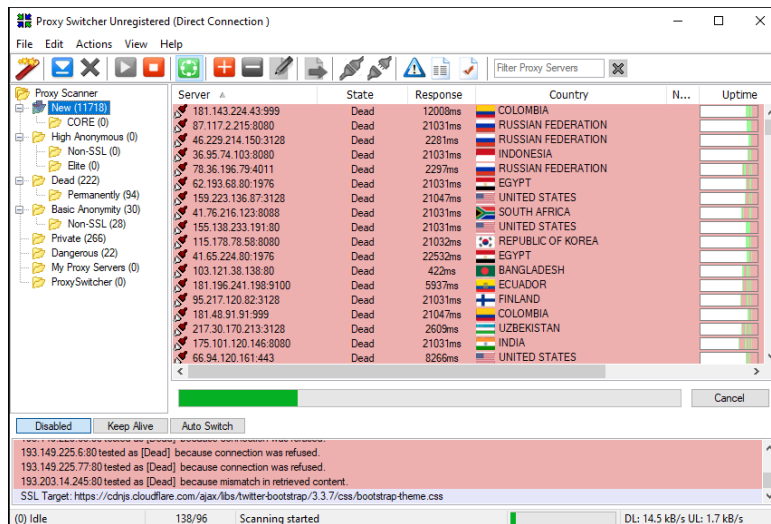
Which tool did you use to find the above information?

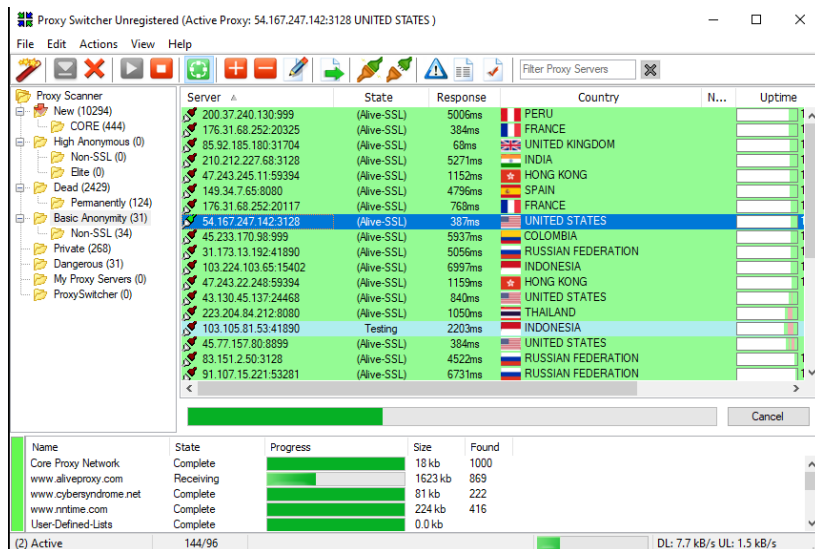
5. Use Proxy Switcher:

- List the available Proxies: Use Common Tasks wizard to find new servers.



- Select any one of the servers from the basic anonymity list and connect to the server. In this example, the connect was made using an available US Server. Make sure you select any available server in Alive-SSL State.

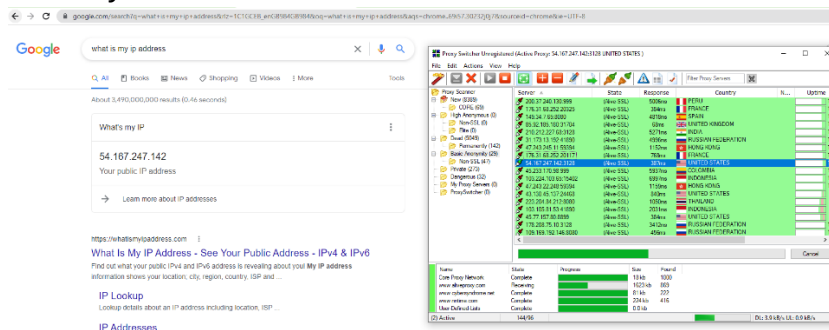




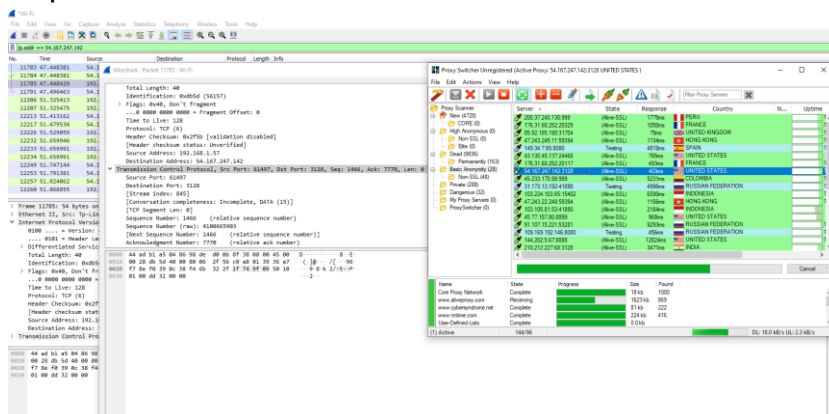
c. Make sure you are connected: Use Proxy Switcher to check your connection.



d. Check your IP Address.



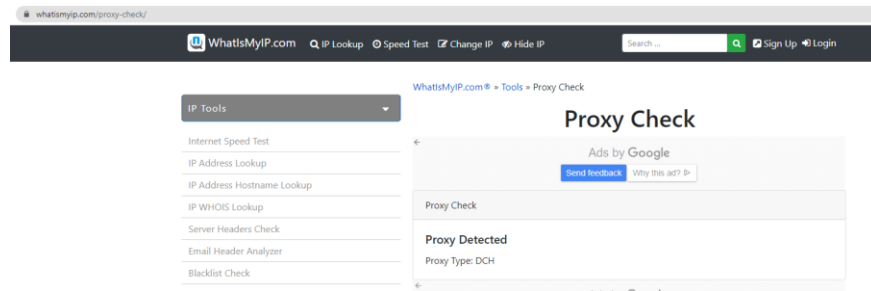
e. Capture Traffic and Check.



6. Use tools, that you have used so far during information-gathering phase to further analyse. What did you get? Did you manage to identify your proxy server or type?



7. Use Whatismyip.com to check your Proxy. What do you see?



8. Based on your usage of this tool, and the analysis done, write your understanding on using Proxy tools like this. Referring to the above screenshot, what is the Proxy type DCH?



Part 6: Identify Target Operating System with TTL

Machine: Windows Servers 2016, Windows 10, Ubuntu, Kali Linux.

Use Wireshark to capture the packets from the target machine and observe TTL, TCP Window Size to determine the Operating System.

Task

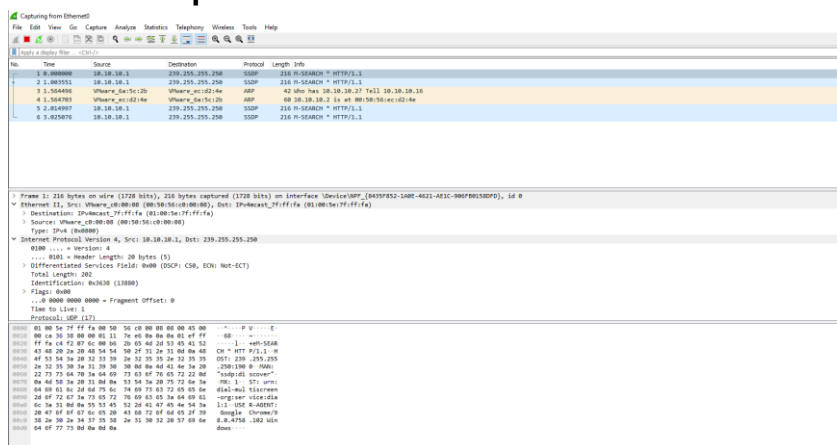
- Before starting this task, you need to know the TTL & TCP Window Size values of different Operating Systems. With reference to our discussion during our lectures,

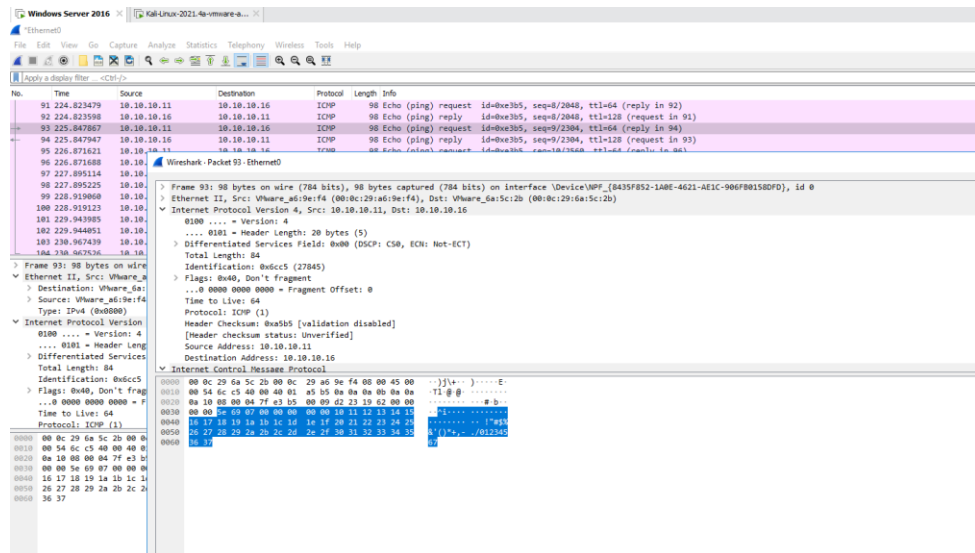
- What is TCP Window Size?
- List out the values below.



Windows	TTL:	TCP WS:
Linux	TTL:	TCP WS:
FreeBSD	TTL:	TCP WS:
Server 2016	TTL:	TCP WS:
Cisco Router (IOS 15.9)	TTL:	TCP WS:

- Login to Win Server 2016. Use Packet Capturing tool and start capturing packets.
- Ping Win Server 2016 from Windows 10, Ubuntu and Kali Linux Machines (Assuming they are the target machines)
- Observe the captured packets in Win Server 2016.
 - Select icmp packets from each target machines to the Server and look for the packet details.





c. From the above output, could you determine what is the Operating System running in 10.10.10.11 host machine?

d. What details did you gather?



e. What assumptions could be made with the gathered information?

Part 7: Map your Network

Machine: Windows Servers 2016, Windows 10, Windows 8.

Map your network using Automatic Mapping Tool.

Task

1. Download Network Topology Mapper from Solarwinds. (You may use different tool to accomplish this task)

Which link did you use to download the tool? Why?

What is the purpose of this tool?



solarwinds.com/network-management-software

IP address management software designed to save time and prevent costly errors • Automated IP address tracking • Integrated DHCP, DNS, and IP address management tools • IP alerting, troubleshooting, and reporting DOWNLOAD FREE TRIAL Quick View Fully functional for 30 days	Network device tracking software designed to locate users and devices on your network • Quickly locate network devices • Map and monitor WAPs, switches, and ports • Manage switch and switch port capacity DOWNLOAD FREE TRIAL Quick View Fully functional for 30 days	VoIP monitoring software designed for deep critical call QoS metrics and WAN performance insights • Real-time WAN monitoring • Troubleshoot VoIP call quality problems • Visual VoIP call path trace DOWNLOAD FREE TRIAL Quick View Fully functional for 30 days
Network Automation Manager Network automation software designed for on-prem, cloud, and hybrid environments • Network performance monitoring • Traffic and bandwidth analysis • Config and change management DOWNLOAD FREE TRIAL Quick View Fully functional for 30 days	Log Analyzer Easily investigate machine data to help identify the root cause of IT issues faster • Log and event collection and analysis • Powerful search and filter • Real-time log stream DOWNLOAD FREE TRIAL Quick View Fully functional for 30 days	Network Topology Mapper Network mapping software built to automatically plot your network • Automate device discovery and mapping • Build multiple maps from a single scan • Perform multi-level network discovery DOWNLOAD FREE TRIAL Quick View Free for 14 days

2. Install the tool in Windows Server 2016.

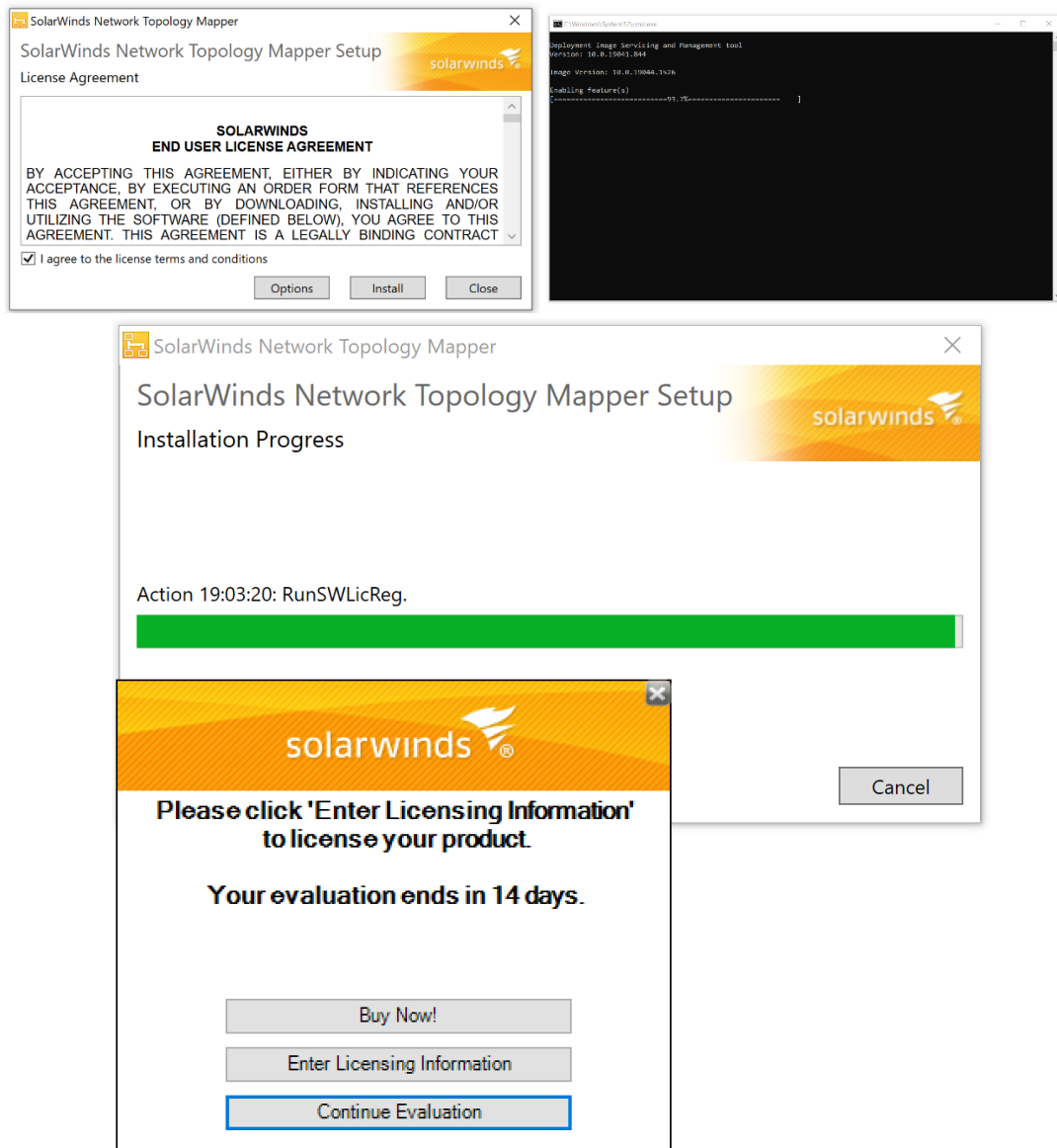
SolarWinds Registration

Orion solarwinds

E-mail Address:

[Continue](#) [Cancel](#)

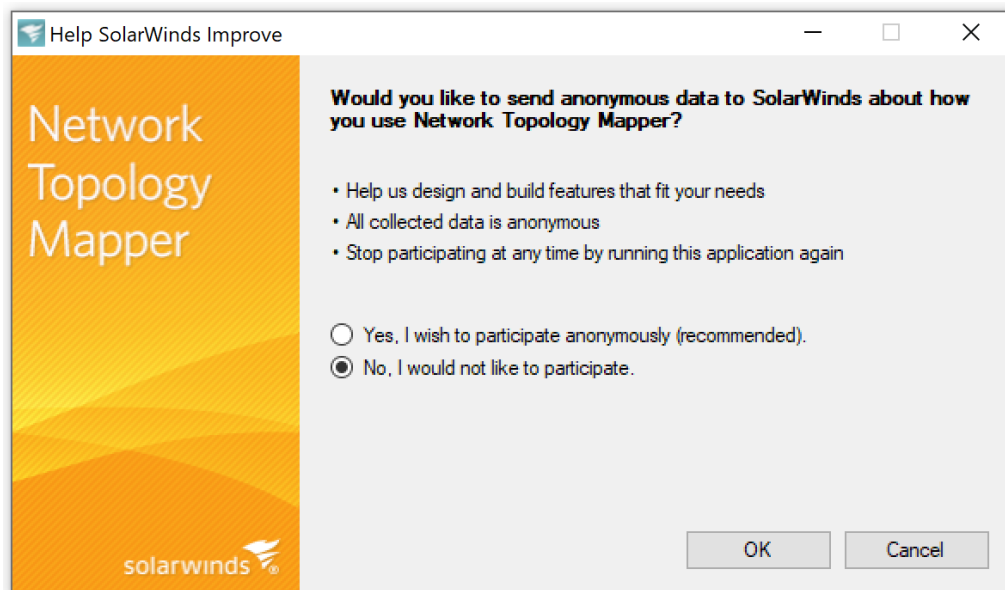
Please confirm the email address you provided when registering to download NTM. If it is blank, please provide your preferred e-mail address. This will help us assist you with pre-sales technical support, educational material, and other account related communications. Installation requires a valid email address.



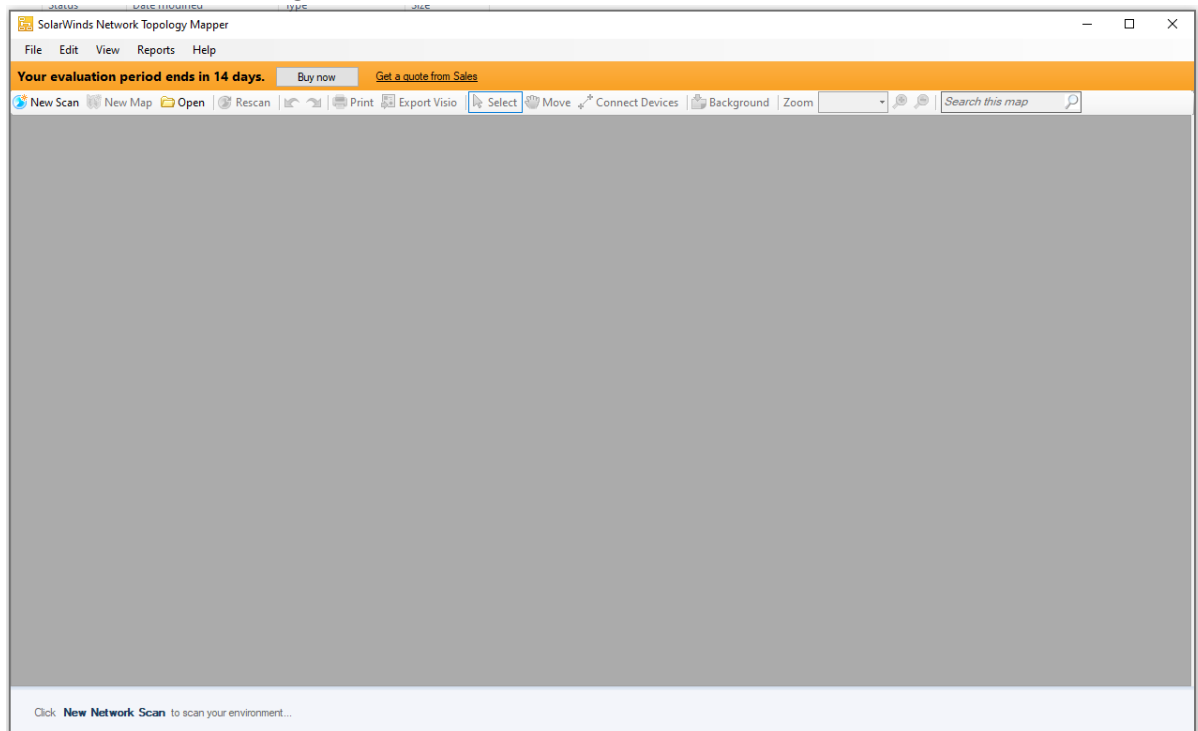
If you are using Network Topology Mapper from Solarwinds,
a) what option did you select on the following “Would you like to send anonymous data to SolarWinds about how you use Network Topology Mapper?”

b) Why did you select the stated option?

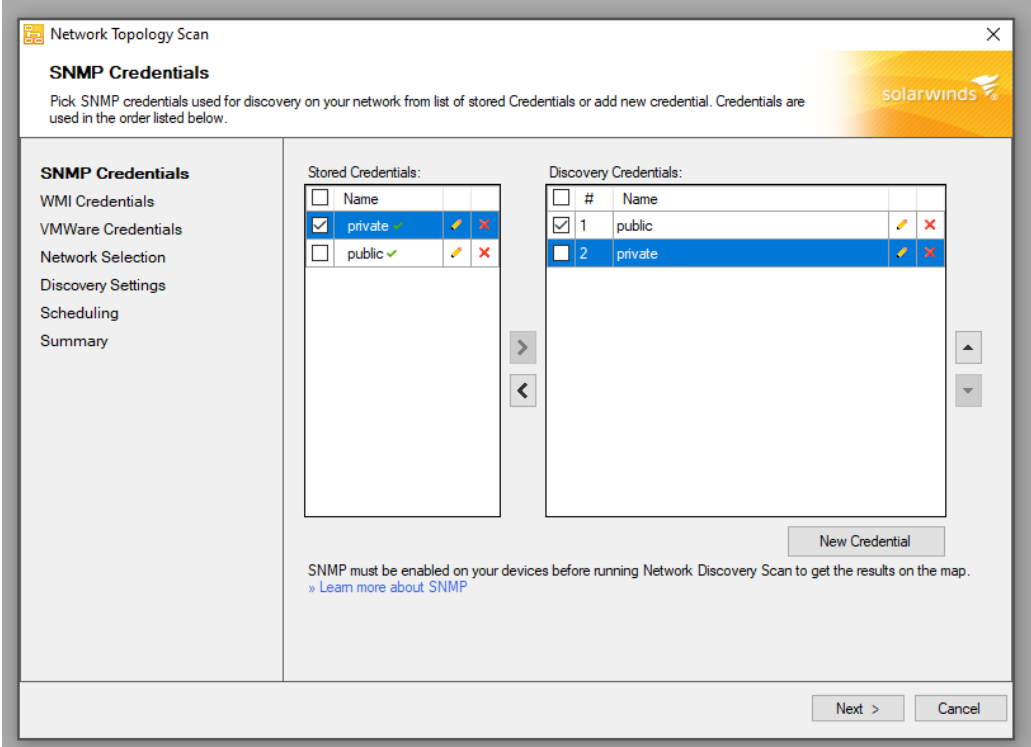




3. After Installation, begin a New Scan



4. Select SNMP Credentials and Select the Network.



Network Topology Scan

SNMP Credentials

Pick SNMP credentials used for discovery on your network from list of stored Credentials or add new credential. Credentials are used in the order listed below.

SNMP Credentials

- WMI Credentials
- VMWare Credentials
- Network Selection**
- Discovery Settings
- Scheduling
- Summary

Stored Credentials:

☐	Name		
☒	private ✓		
☐	public ✓		

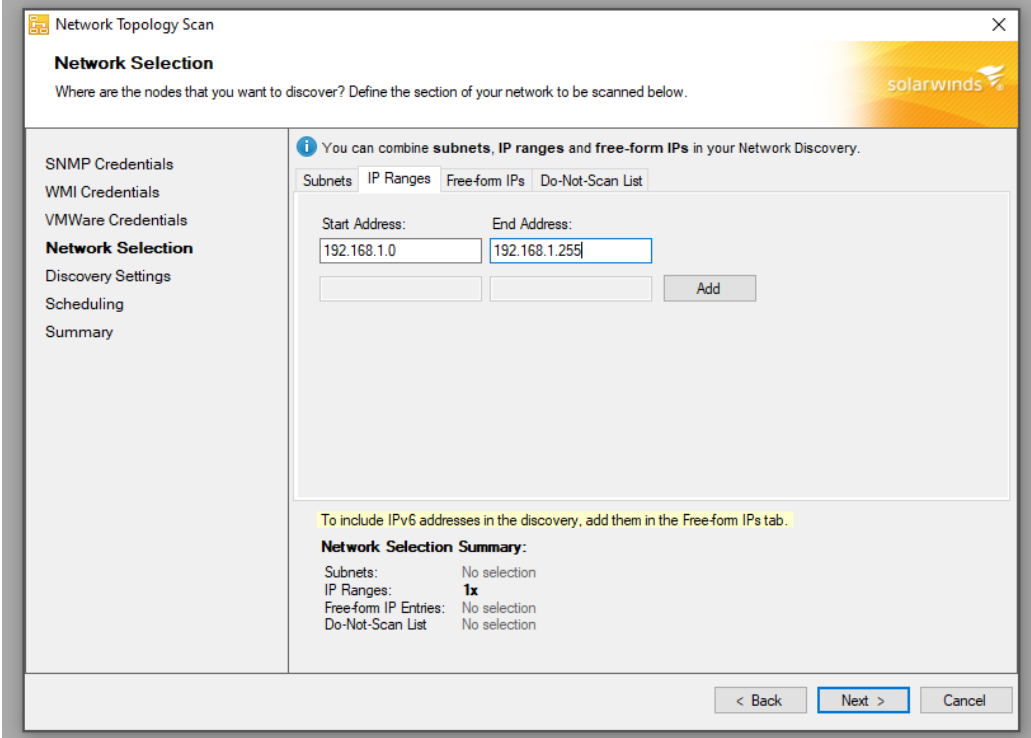
Discovery Credentials:

☐	#	Name		
☒	1	public		
☐	2	private		

New Credential

SNMP must be enabled on your devices before running Network Discovery Scan to get the results on the map.
[» Learn more about SNMP](#)

Next > Cancel



Network Topology Scan

Network Selection

Where are the nodes that you want to discover? Define the section of your network to be scanned below.

SNMP Credentials

- WMI Credentials
- VMWare Credentials
- Network Selection**
- Discovery Settings
- Scheduling
- Summary

Subnets IP Ranges Free-form IPs Do-Not-Scan List

Start Address: 192.168.1.0 **End Address:** 192.168.1.255

Add

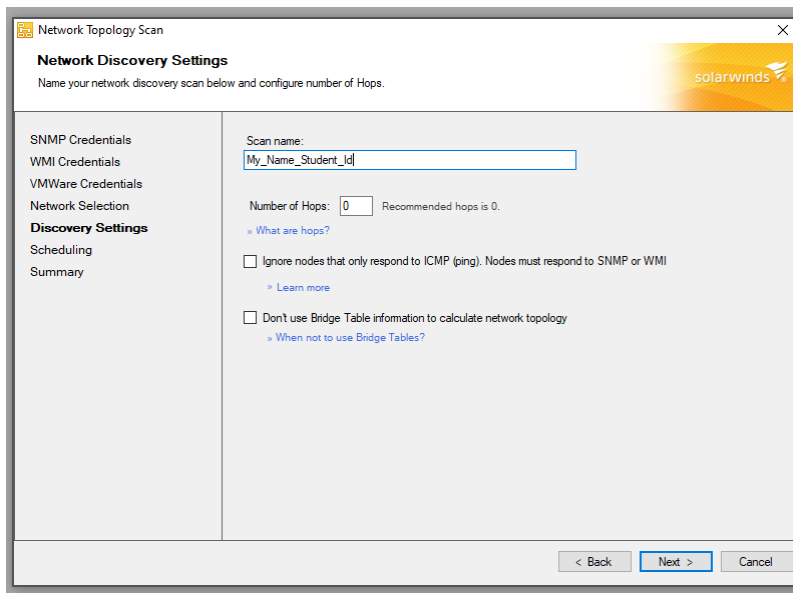
To include IPv6 addresses in the discovery, add them in the Free-form IPs tab.

Network Selection Summary:

Subnets:	No selection
IP Ranges:	1x
Free-form IP Entries:	No selection
Do-Not-Scan List:	No selection

< Back Next > Cancel

5. Assign your name and Student Id as the Name to Scan and Discover the network.



Network Topology Scan

Network Discovery Settings

Name your network discovery scan below and configure number of Hops.

SNMP Credentials
WMI Credentials
VMWare Credentials
Network Selection
Discovery Settings
Scheduling
Summary

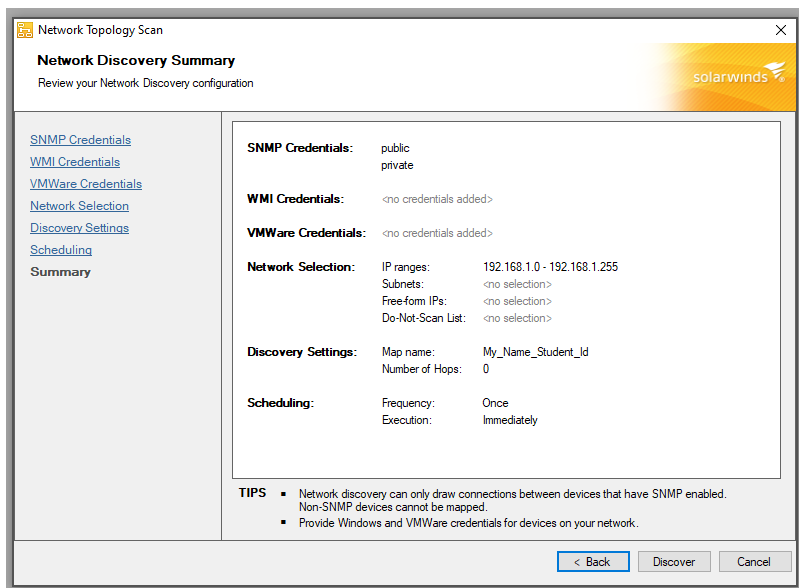
Scan name:

Number of Hops: Recommended hops is 0.
[» What are hops?](#)

☐ Ignore nodes that only respond to ICMP (ping). Nodes must respond to SNMP or WMI
[» Learn more](#)

☐ Don't use Bridge Table information to calculate network topology
[» When not to use Bridge Tables?](#)

< Back Next > Cancel



Network Topology Scan

Network Discovery Summary

Review your Network Discovery configuration

[SNMP Credentials](#)
[WMI Credentials](#)
[VMWare Credentials](#)
[Network Selection](#)
[Discovery Settings](#)
[Scheduling](#)
Summary

SNMP Credentials: public
private

WMI Credentials: <no credentials added>

VMWare Credentials: <no credentials added>

Network Selection: IP ranges: 192.168.1.0 - 192.168.1.255
Subnets: <no selection>
Free-form IPs: <no selection>
Do-Not-Scan List: <no selection>

Discovery Settings: Map name: My_Name_Student_Id
Number of Hops: 0

Scheduling: Frequency: Once
Execution: Immediately

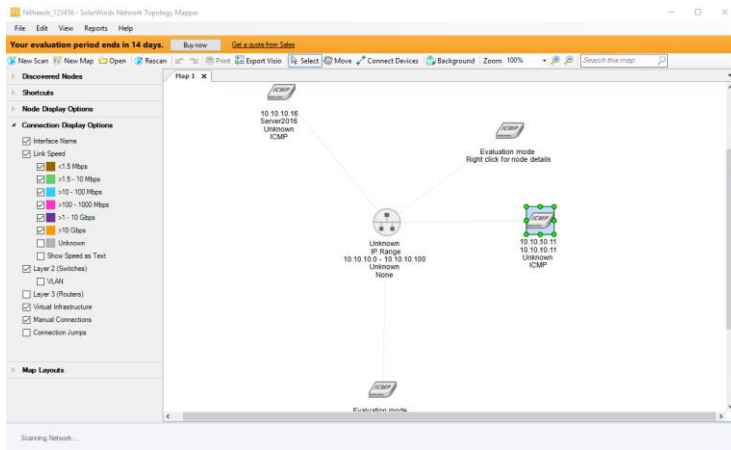
TIPS

- Network discovery can only draw connections between devices that have SNMP enabled. Non-SNMP devices cannot be mapped.
- Provide Windows and VMWare credentials for devices on your network.

< Back Discover Cancel

/ In my case, I have used 192.168.1.0 range of IP Address.*

6. Use the details to map your network. You will now have a network topology. Expand and explore the Node Display Options, Map Layouts to gather more information. */* In my case, I have used 10.10.10.0 range of IP Address.*



7. Use Integration with Windows Tools to gain access using Remote Desktop, gather more information using ping, traceroute, Telnet etc.

8. Generate Report

Nitheesh_123456 - Inventory report

Export Print Options

IP Address	IP Addresses	Hostname	Primary Role	Roles	Sysname	Machine Type	Vendor	Location	Contact	System Description	Polling Method	MAC Addresses
10.10.10.2	10.10.10.2	10.10.10.2	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.8	10.10.10.8	WIN-4L1UT...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.10	10.10.10.10	DESKTOP-G...	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.11	10.10.10.11	10.10.10.11	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
10.10.10.16	10.10.10.16	Server2016	ICMP Node	ICMP N...		Unknown	Unknown				ICMP	
		IP Range10...	Network Segm...	Network...		Unknown	Unknown				None	

With reference to our lectures, enumeration when you try and connect to the system and do deliberate actions to gather more information. The initial process of enumeration includes finding names of the machines within Target network. Using the gathered names, detailed information on network and its resources could be probed.

Part 8: Enumerate using NetBIOS

Machine: Windows Servers 2016, Windows Server 2012.

Using tools like Global Network Inventory is used to scan the networks based on IP range, Domain, Host etc.

Task

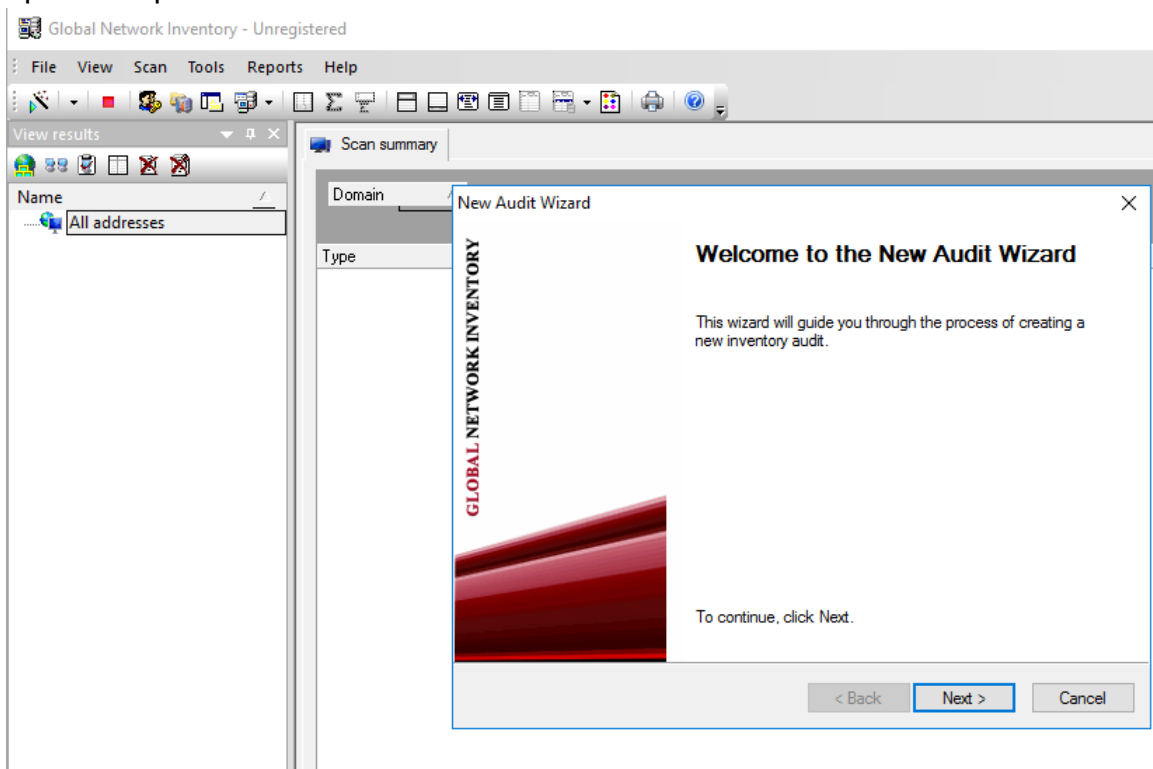
1. Download Global Network Inventory tool. (You may use different tool to accomplish this task)

Which link did you use to download the tool? Why?

What is the purpose of this tool?



2. Install GNI tool. Open the New Audit Wizard and initiate the scan. You have two options to proceed further.

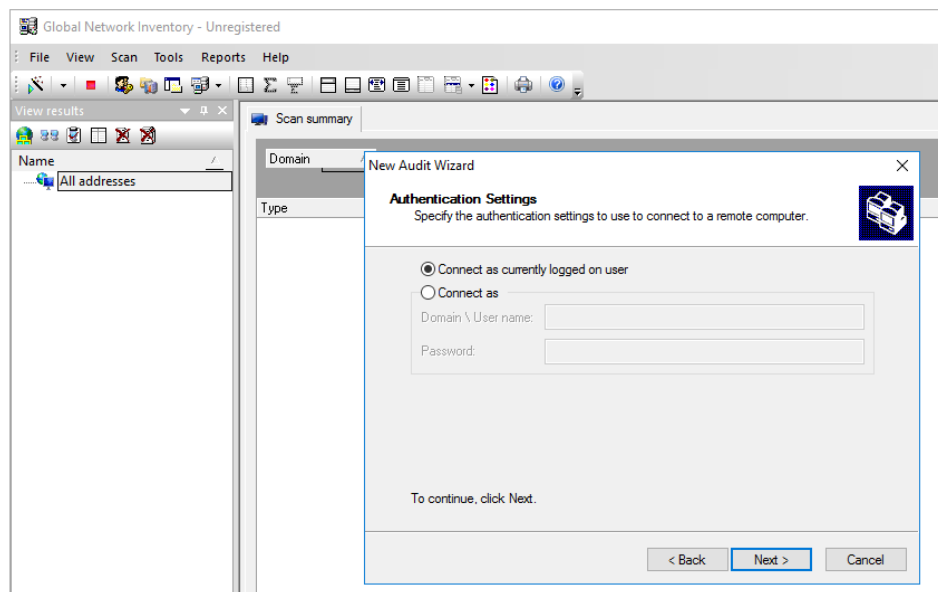


a. Connect as currently logged on user

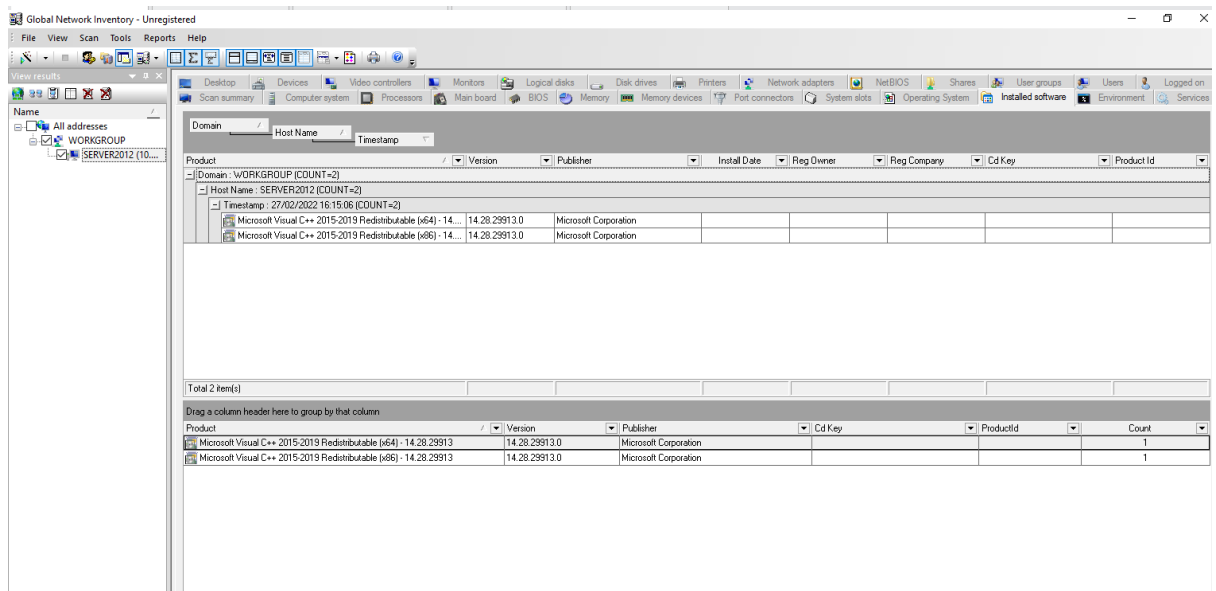
If you are using this tool in an initial stage where you don't have the user credentials of the target, use this option. However, by using this option you might only get basic information like Physical and Logical addresses.

b. Connect as

Once you have managed to get the user credentials of the target, use that and connect as the target and gather information.



3. Do scans using both the options and gather as many information as possible.



What is the difference between both the scans?



Using user credentials, did you manage to gather information like Software's Installed, Services Running, NetBIOS information, Users, User Groups, Operating System etc?

Yes!! – What is your gathered information?

No!! – Why? Reason out and do research, troubleshoot, and gather the above information.

4. Generate Report

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali-Linux-2021.4a-vmware-a...

Global Network Inventory Services | February 27, 2022

visit <http://www.magnetosoft.com> for sales and support.

Services

Name	Start Type	State	File
Domain: WORKGROUP (COUNT=156)			
Host Name: SERVER2012 (COUNT=156)			
Timestamp: 27/02/2022 16:15:06 (COUNT=156)			
App Readiness	Manual	Stopped	C:\Windows\System32\svchost.exe -k AppReadiness
Application Experience	Manual	Running	C:\Windows\system32\svchost.exe -k netsvcs
Application Host Helper Service	Automatic	Running	C:\Windows\system32\svchost.exe -k apphost
Application Identity	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted
Application Information	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
Application Layer Gateway Service	Manual	Stopped	C:\Windows\System32\alg.exe
Application Management	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
AppX Deployment Service (AppXSVC)	Manual	Stopped	C:\Windows\system32\svchost.exe -k wsappx
ASP.NET State Service	Manual	Stopped	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe
Background Intelligent Transfer Service	Manual	Stopped	C:\Windows\System32\svchost.exe -k netsvcs
Background Tasks Infrastructure Service	Automatic	Running	C:\Windows\system32\svchost.exe -k DcomLaunch
Base Filtering Engine	Automatic	Running	C:\Windows\system32\svchost.exe -k LocalServiceNetwork
BranchCache	Automatic	Running	C:\Windows\System32\svchost.exe -k PeerDist
Certificate Propagation	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
Client for NFS	Automatic	Running	C:\Windows\system32\ntfsdnt.exe
CNG Key Isolation	Manual	Stopped	C:\Windows\system32\lsass.exe
COM+ Event System	Automatic	Running	C:\Windows\system32\svchost.exe -k LocalService
COM+ System Application	Manual	Running	C:\Windows\system32\clbcatq.exe {02D4B3F1-FD88-11D1-86D0-00805FC79235}
Credential Manager	Disabled	Stopped	C:\Windows\System32\svchost.exe -k netsvcs
Cryptographic Services	Manual	Stopped	C:\Windows\system32\lsass.exe
DCOM Server Process Launcher	Automatic	Running	C:\Windows\system32\svchost.exe -k NetworkService
Device Association Service	Automatic	Running	C:\Windows\system32\svchost.exe -k DcomLaunch
Device Install Service	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted
Device Setup Manager	Manual	Stopped	C:\Windows\system32\svchost.exe -k netsvcs
DHCP Client	Automatic	Running	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted
Diagnostic Policy Service	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalServiceNetwork
Diagnostic Service Host	Manual	Stopped	C:\Windows\system32\svchost.exe -k LocalService
Diagnostic System Host	Manual	Running	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
Distributed Link Tracking Client	Automatic	Running	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali-Linux-2021.4a-vmware-a...

Global Network Inventory Desktop | February 27, 2022

visit <http://www.magnetosoft.com> for sales and support.

Desktop

Screen Saver Executable	Screen Saver Active	Screen Saver Secure	Screen Saver Timeout, min
Domain: WORKGROUP (COUNT=7)			
Host Name: SERVER2012 (COUNT=7)			
Timestamp: 27/02/2022 16:15:06 (COUNT=7)			
Name: DEFAULT (COUNT=1)			
Name: IIS APPPOOL\NET v4.5 (COUNT=1)	No	No	0
Name: IIS APPPOOL\NET v4.5 Classic (COUNT=1)	No	No	0
Name: NT AUTHORITY\LOCAL SERVICE (COUNT=1)	No	No	0
Name: NT AUTHORITY\NETWORK SERVICE (COUNT=1)	No	No	0
Name: NT AUTHORITY\SYSTEM (COUNT=1)	No	No	0
Name: SERVER2012\Administrator (COUNT=1)	No	No	0
Total 7 item(s)	No	No	0

Windows Server 2016 x Windows Server 2012 x Windows 10 and later x64 x Windows 8.x x64 x Kali-Linux-2021.4a-vmware-a...

Global Network Inventory Network adapters | February 27, 2022

visit <http://www.magnetosoft.com> for sales and support.

Network adapters

Adapter Name	MAC Address	Adapter IP Address	Adapter IP Subnet	Adapter Default IP Gateway	Manufacturer	Adapter Type	DHCP Enabled
Domain: WORKGROUP (COUNT=1)							
Host Name: SERVER2012 (COUNT=1)							
Timestamp: 27/02/2022 16:15:06 (COUNT=1)							
Intel(R) 82574L Gigabit Network Connection	00:0C:29:6C:7C:49	10.10.10.12	255.255.255.0	10.10.10.2	Intel Corporation	Ethernet 802.3	No
Total 1 item(s)							

5. What are the other similar tools did you manage to research? Could you compare those tools with this and discuss the pros and cons?



Part 9: Enumerate using Nmap and Net Use

Machine: Windows Servers 2016, Windows Server 2012, Win 10, Win 8, Win XP.
(If you don't have all these machines, you can do this activity with a minimum of 2 windows machines)

Using this technique, we could gather User names, User groups, List of Computers, OS, Ports, Names, Network resources, Services, Policies and Passwords

Task

1. Download and Install Nmap in Win Server 2012.

Which link did you use to download the tool? Why?

What is the purpose of this tool?



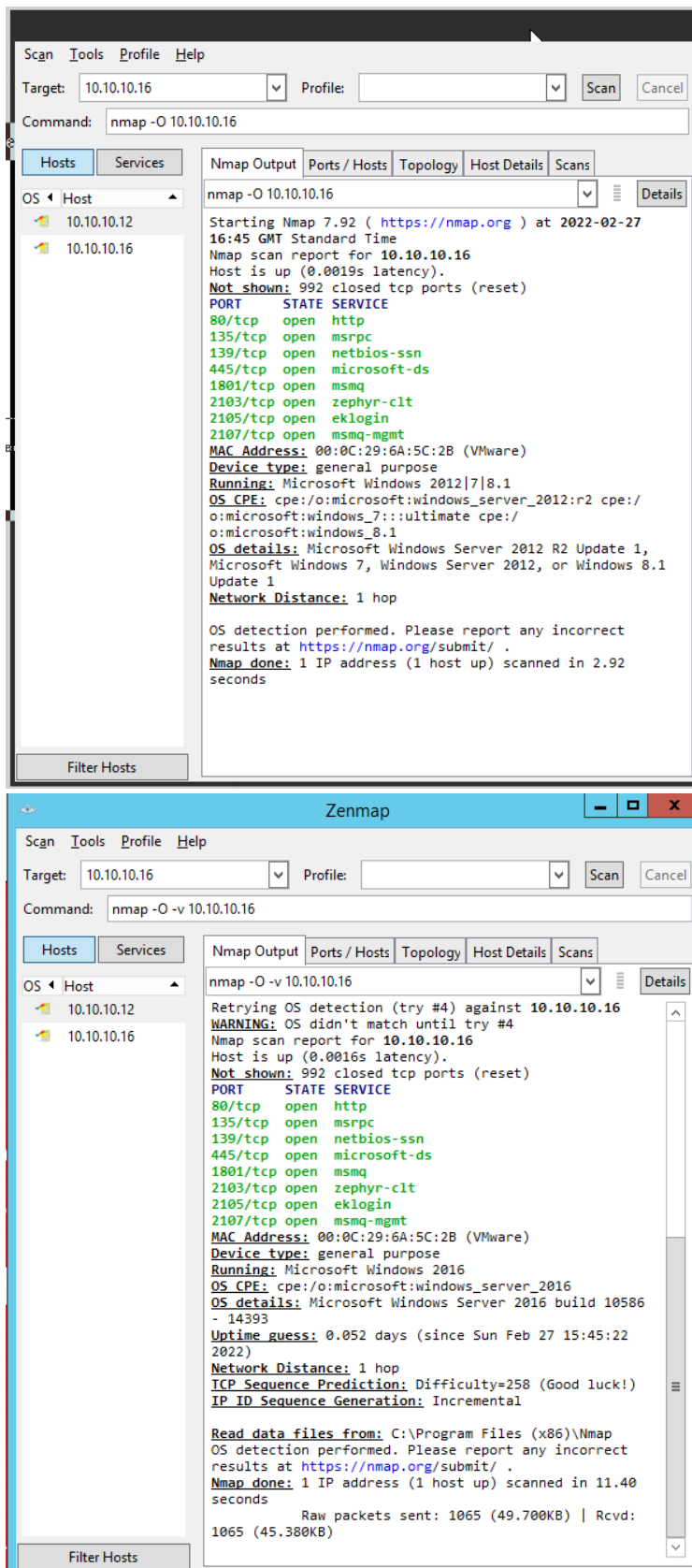
2. By default, you could see an Intense scan profile present. Do various scans on the target OS. Refer to our lecture sessions to use various nmap commands.
3. Based on the earlier activities, we have managed to find our Users, Host Names, Live Hosts, List of Machines in the Target Network etc. Now, let us focus on gathering ports open, their services and shared resources.
4. Issue the nmap command to find out the operating system. Which command would you use?

Nmap -O <Target>

Nmap -O -v <Target>

what is the difference between the above two commands?





5. From the above output/ or from your output, what is your finding? Did you notice Ports 80, 135, 139, 445, 1801 etc are open and 139 is using netbios service? Let us use NBTSTAT command to look at NETBIOS related information.

NBTSTAT is a diagnostic tool for NetBIOS over TCP/IP. It's primary objective is to troubleshoot NetBIOS name resolution problems. (Wikipedia)

```
C:\Users\Administrator>nbtstat -A 10.10.10.16
```

```
Ethernet0:
```

```
Node IpAddress: [10.10.10.12] Scope Id: []
```

NetBIOS Remote Machine Name Table

Name	Type	Status
SERVER2016	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
SERVER2016	<20> UNIQUE	Registered

```
MAC Address = 00-0C-29-6A-5C-2B
```

```
C:\Users\Administrator>nbtstat -A 10.10.10.12
```

```
Ethernet0:
```

```
Node IpAddress: [10.10.10.12] Scope Id: []
```

NetBIOS Remote Machine Name Table

Name	Type	Status
SERVER2012	<00> UNIQUE	Registered
WORKGROUP	<00> GROUP	Registered
SERVER2012	<20> UNIQUE	Registered

```
MAC Address = 00-0C-29-6C-7C-49
```

6. Now use net use command to view the created shared folders from your hosts.

```
C:\Users\Administrator>net use
New connections will be remembered.
```

Status	Local	Remote	Network
	Z:	\\vmware-host\Shared Folders	VMware Shared Folders

The command completed successfully.

7. Do research on net use. Know what is the purpose of net use command? Which OS versions is that supported?



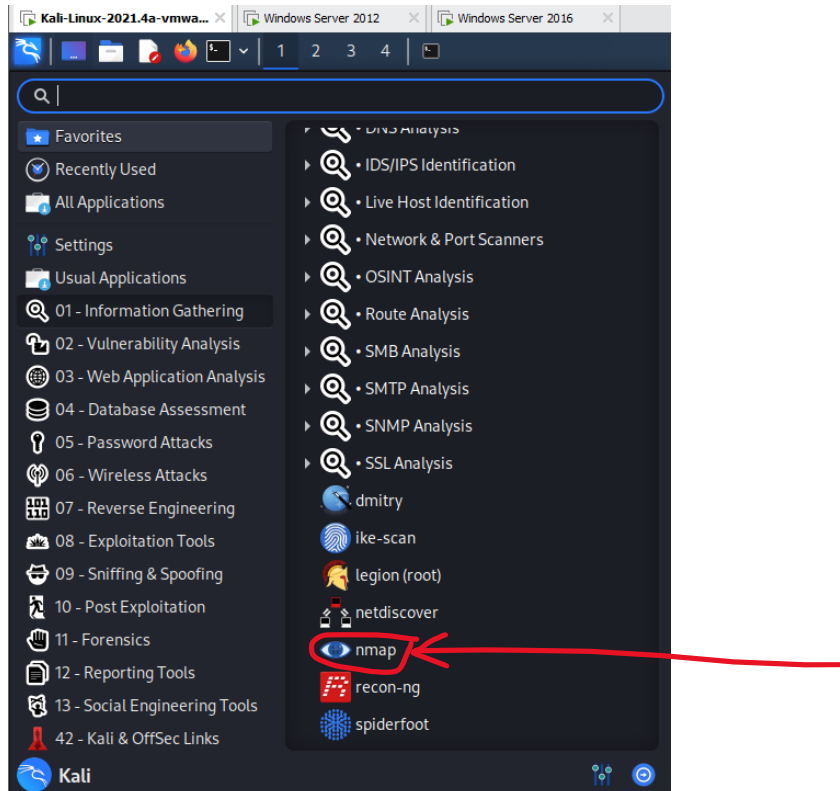
Part 10: Enumerate Services

Machine: Windows Servers 2016, Windows Server 2012, Kali.

Scan all the machines in the target network, list out the up and running machines, find open ports, find the status of firewall and enumerate the services running on the port along with their versions.

Task

1. Download and Install Nmap in Win Server 2012.



2. Execute the commands
 - a. **nmap -sP 10.10.10.0/24**

```
(kali㉿kali)-[~]  
$ nmap -sP 10.10.10.0/24  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:23 EST  
Nmap scan report for 10.10.10.2  
Host is up (0.00093s latency).  
Nmap scan report for 10.10.10.11  
Host is up (0.0020s latency).  
Nmap scan report for 10.10.10.12  
Host is up (0.0039s latency).  
Nmap scan report for 10.10.10.16  
Host is up (0.0019s latency).  
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.53 seconds
```

This lab activity has a number of nmap commands. Could you list out all the descriptions of these commands?

For example, the 1st command used here is **nmap -sP 10.10.10.0/24**

What is the purpose of this command? This scan lists the hosts that responded to the ping within the specified range of IP addresses. By using



this command, you could determine the status like up and live hosts in the target network. This is also known as Ping sweeping.

b. Nmap -sS 10.10.10.12

```

# nmap -sS 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:29 EST
Nmap scan report for 10.10.10.12
Host is up (0.00049s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1027/tcp  open  IIS
1028/tcp  open  unknown
1029/tcp  open  ms-lsa
1030/tcp  open  iad1
1031/tcp  open  iad2
1032/tcp  open  iad3
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt

```

Nmap -sS <target> scan is a

c. nmap -ssV -O 10.10.10.12

```

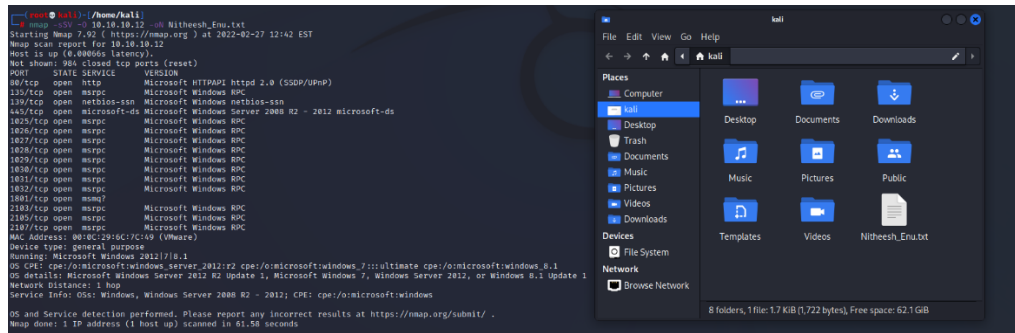
(root@kali)-[/home/kali]
# nmap -ssV -O 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:36 EST
Nmap scan report for 10.10.10.12
Host is up (0.00047s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft
-ds
1025/tcp  open  msrpc       Microsoft Windows RPC
1026/tcp  open  msrpc       Microsoft Windows RPC
1027/tcp  open  msrpc       Microsoft Windows RPC
1028/tcp  open  msrpc       Microsoft Windows RPC
1029/tcp  open  msrpc       Microsoft Windows RPC
1030/tcp  open  msrpc       Microsoft Windows RPC
1031/tcp  open  msrpc       Microsoft Windows RPC
1032/tcp  open  msrpc       Microsoft Windows RPC
1801/tcp  open  msmq?
2103/tcp  open  msrpc       Microsoft Windows RPC
2105/tcp  open  msrpc       Microsoft Windows RPC
2107/tcp  open  msrpc       Microsoft Windows RPC
MAC Address: 00:0C:29:6C:7C:49 (VMware)
Device type: general purpose
Running: Microsoft Windows 2012|7|8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7:::ultimate cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, W
indows Server 2012, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 79.12 seconds

```

nmap -ssV -O <target> scan is a

- d. Save this report to a txt file with your name. What command do you use to save?

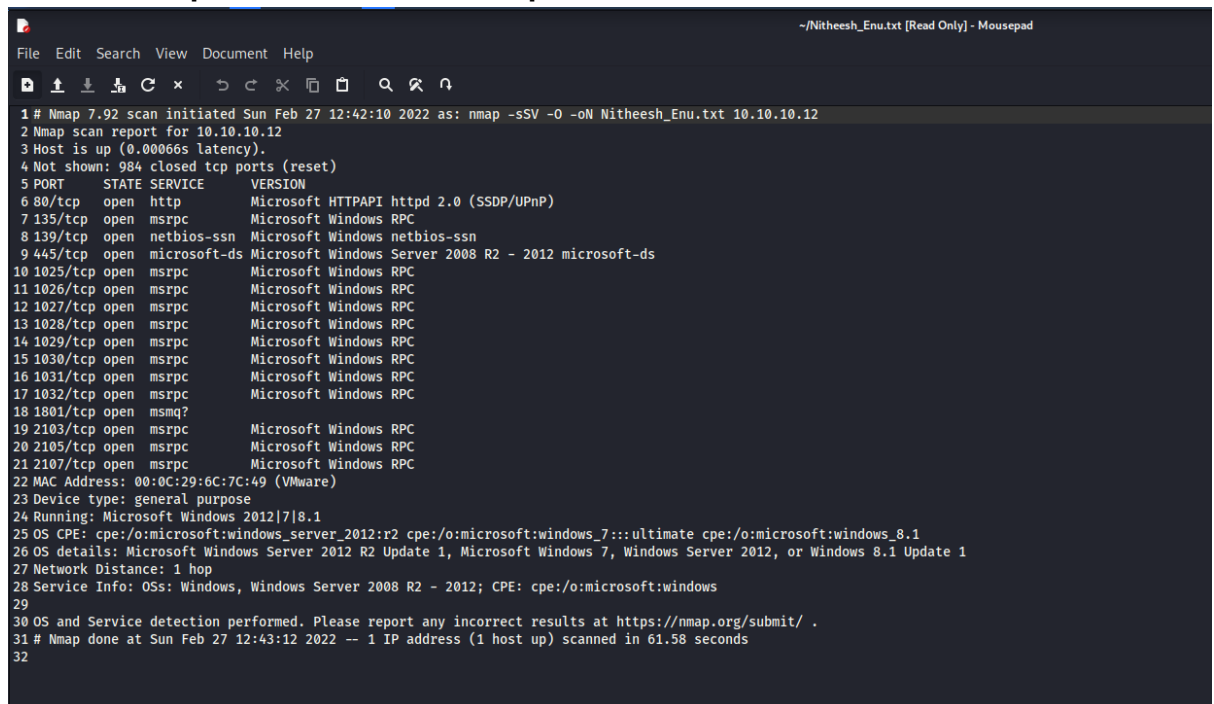


```

root@kali: ~/Documents
└─$ nmap -sV -oN Nitheesh_Enu.txt
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:42 EST
Nmap scan report for 10.10.10.12
Host is up (0.00066s latency).
Not shown: 984 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
135/tcp   open  msrpc     Microsoft Windows RPC
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1025/tcp  open  msrpc     Microsoft Windows RPC
1026/tcp  open  msrpc     Microsoft Windows RPC
1027/tcp  open  msrpc     Microsoft Windows RPC
1028/tcp  open  msrpc     Microsoft Windows RPC
1029/tcp  open  msrpc     Microsoft Windows RPC
1030/tcp  open  msrpc     Microsoft Windows RPC
1031/tcp  open  msrpc     Microsoft Windows RPC
1032/tcp  open  msrpc     Microsoft Windows RPC
1801/tcp  open  msmq?     Microsoft Windows RPC
2103/tcp  open  msrpc     Microsoft Windows RPC
2105/tcp  open  msrpc     Microsoft Windows RPC
2107/tcp  open  msrpc     Microsoft Windows RPC
MAC Address: 00:0C:29:6C:7C:49 (VMware)
Device type: general purpose
Running: Microsoft Windows 2012/7/8.1
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.58 seconds

```

3. Save the Report and submit the report.



```

~/.Nitheesh_Enu.txt [Read Only] - Mousepad
File Edit Search View Document Help
1 # Nmap 7.92 scan initiated Sun Feb 27 12:42:10 2022 as: nmap -sV -oN Nitheesh_Enu.txt 10.10.10.12
2 Nmap scan report for 10.10.10.12
3 Host is up (0.00066s latency).
4 Not shown: 984 closed tcp ports (reset)
5 PORT      STATE SERVICE VERSION
6 80/tcp    open  http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7 135/tcp   open  msrpc     Microsoft Windows RPC
8 139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
9 445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
10 1025/tcp  open  msrpc     Microsoft Windows RPC
11 1026/tcp  open  msrpc     Microsoft Windows RPC
12 1027/tcp  open  msrpc     Microsoft Windows RPC
13 1028/tcp  open  msrpc     Microsoft Windows RPC
14 1029/tcp  open  msrpc     Microsoft Windows RPC
15 1030/tcp  open  msrpc     Microsoft Windows RPC
16 1031/tcp  open  msrpc     Microsoft Windows RPC
17 1032/tcp  open  msrpc     Microsoft Windows RPC
18 1801/tcp  open  msmq?     Microsoft Windows RPC
19 2103/tcp  open  msrpc     Microsoft Windows RPC
20 2105/tcp  open  msrpc     Microsoft Windows RPC
21 2107/tcp  open  msrpc     Microsoft Windows RPC
22 MAC Address: 00:0C:29:6C:7C:49 (VMware)
23 Device type: general purpose
24 Running: Microsoft Windows 2012/7/8.1
25 OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_7::ultimate cpe:/o:microsoft:windows_8.1
26 OS details: Microsoft Windows Server 2012 R2 Update 1, Microsoft Windows 7, Windows Server 2012, or Windows 8.1 Update 1
27 Network Distance: 1 hop
28 Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
29
30 OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
31 # Nmap done at Sun Feb 27 12:43:12 2022 -- 1 IP address (1 host up) scanned in 61.58 seconds
32

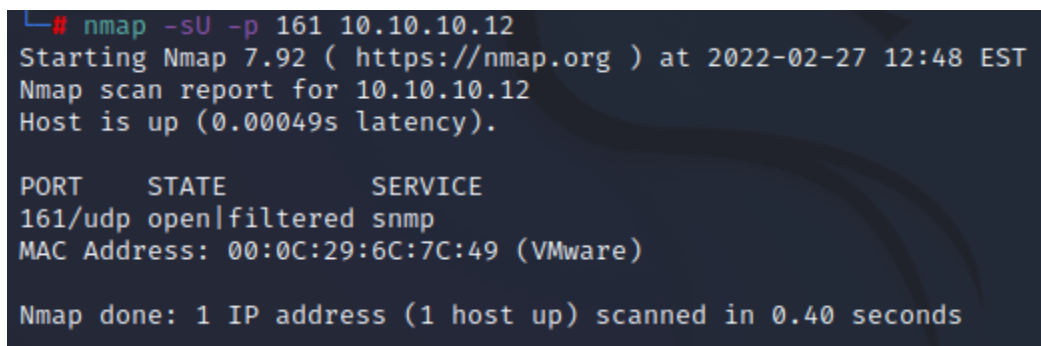
```

4. Now, let us focus on SNMP.

Which is the default port for SNMP?



- a. Check the port status.



```

└─$ nmap -sU -p 161 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 12:48 EST
Nmap scan report for 10.10.10.12
Host is up (0.00049s latency).

PORT      STATE SERVICE
161/udp    open|filtered snmp
MAC Address: 00:0C:29:6C:7C:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds

```

- b. From the above output, knowing that SNMP Service is running in port 161 and the status is open, execute a script to extract the SNMP Community string from the target machine.

```
# nmap -sU -p 161 --script=snmp-brute 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 13:22 EST
Nmap scan report for 10.10.10.12
Host is up (0.00042s latency).

PORT      STATE      SERVICE
161/udp    open|filtered snmp
MAC Address: 00:0C:29:6C:7C:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.78 seconds
```

```
(root@kali)-[/home/kali]
# nmap -sU -p 161 --script=snmp-brute 10.10.10.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-27 13:24 EST
Nmap scan report for 10.10.10.12
Host is up (0.00056s latency).

PORT      STATE SERVICE
161/udp    open  snmp
| snmp-brute:
|_ public - Valid credentials
MAC Address: 00:0C:29:6C:7C:49 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

Above two commands are same but outputs are different. Could you justify why the outputs are different? What actions was taken before executing the command second time?



- c. With valid credentials, let us perform SNMP enumeration on the target machine.

5. Open MSFCONSOLE



Know about MSF console. Do research on Metasploit. A very useful tool in Kali Linux. Refer to Metasploit.com, Github for references.



- a. Use `auxiliary/scanner/snmp/snmp_login`. Setg `RHOSTS <target>`. Exploit.

```
msf6 > use auxiliary/scanner/snmp/snmp_login
msf6 auxiliary(scanner/snmp/snmp_login) > setg RHOSTS 10.10.10.12
RHOSTS => 10.10.10.12
msf6 auxiliary(scanner/snmp/snmp_login) > exploit

[!] No active DB -- Credential data will not be saved!
[+] 10.10.10.12:161 - Login Successful: public (Access level: read-only); Proof (sysDescr.0): Hardware: Intel64
Family 6 Model 158 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 Multiprocessor Free
)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Did you notice that the target has a read-only community string? *(If you don't understand SNMP Community String – refer to our lectures and/or do research)*

- b. Use Enumeration to exploit further.

```
msf6 auxiliary(scanner/snmp/snmp_login) > use auxiliary(scanner/snmp/snmp_enum)
msf6 auxiliary(scanner/snmp/snmp_enum) > exploit

[+] 10.10.10.12, Connected.

[*] System information:

Host IP                : 10.10.10.12
Hostname               : Server2012.accb.com
Description            : Hardware: Intel64 Family 6 Model 158 Stepping 9 AT/AT COMPATIBLE - Software: Wi
ndows Version 6.3 (Build 9600 Multiprocessor Free)
Contact                : -
Location               : -
Uptime snmp            : 00:23:23.07
Uptime system          : 00:22:46.53
System date            : 2022-2-27 18:33:18.3

[*] User accounts:

["Guest"]
["krbtgt"]
["Administrator"]

[*] Network information:

IP forwarding enabled  : no
Default TTL            : 128
TCP segments received  : 9320
TCP segments sent      : 9312
TCP segments retrans   : 8
Input datagrams        : 405
```

After enumerating the target on SNMP, what information did you gather?



In similar method, could you try to enumerate LDAP on an ADDS and modify domain user accounts?

Record your Reflection:



1. Understanding on all the activities
2. Understanding about various tools used
3. New/ Similar tools you identified and used
4. Compare and Contrast the tutorial tools with your identified tools
5. Rate yourself: How confident are you to do footprinting and reconnaissance activity ethically?
6. Any other Troubleshooting Steps, you need to share?